IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

IN THE MATTER OF THE SEARCH OF THE PERSON OF TRAVIS R. CHAPELL AND THE PREMISES AT 8900 TEAKWOOD DR., DISPUTANTA, VA 23842	Case No. 3:20sw162 **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Special Agent Michael J. Roelofs being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the person of Travis R. Chapell and his premises known as 8900 Teakwood Dr., Disputanta, VA 23842, including all structures on the property, hereinafter "PREMISES," all as further described Attachment A, for the things described in Attachment B.

2. I am a Special Agent (SA) with the U.S. Army Criminal Investigation Command (USACIDC), and have been employed in that position since November 2011. I am currently assigned to the Major Cybercrime Unit, since June 2017. The Major Cybercrime Unit is responsible for investigating computer-related offenses including child pornography, extortion, computer intrusions, denial of service attacks and other types of malicious computer activity directed against the U.S. Army or conducted using Army computers. I am also a certified DoD Cyber Crime Investigator (CCI), Digital Forensic Examiner (DFE), and Digital Media Collector (DMC). As a special agent, I have personally been the affiant and/or participated in the execution of a number of federal search warrants that have involved child exploitation and/or

child pornography offenses. I have attended the U.S. Army Criminal Investigation Division Special Agent Course (CIDSAC), a federally accredited criminal investigator training program, the Federal Law Enforcement Training Center (FLETC), and completed numerous advanced Special Agent training courses specifically in Digital Forensics and Digital Media Collection. In addition to my training as a criminal investigator, I have received advanced training in cases involving Child Exploitation and I am a member of several Task Forces affiliated to the Internet Crimes Against Children (ICAC) Program. As part of my duties, I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography, in violation of the Uniform Code of Military Justice, as well as, violations of Title 18, United States Code, Sections 2251, 2252, and 2252A. As part of my training and experience, I have reviewed images containing child pornography in a variety of formats (such as digital still images and video images) and media (such as digital storage devices, the Internet, and printed images). As a civilian Special Agent of USACIDC, I am authorized to investigate crimes involving violations of the Uniform Code of Military Justice, and other applicable federal laws, where there is an Army interest.

3. Through my training and experience, I have become familiar with the methods used by people who commit offenses involving the sexual exploitation of children. My training and experience has given me an understanding of how people who commit offenses relating to the sexual exploitation of children use the Internet to facilitate and commit those offenses.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended

to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, § 2252A(a)(2)(A) (receipt and distribution of child pornography), and 2252A(a)(5)(B) (possession of child pornography) have been committed by Travis R. Chapell. There is also probable cause to search the person of Travis R. Chappell and the PREMISES, all further described in Attachment A for evidence and/or instrumentalities of these crimes, as described in Attachment B.

TECHNICAL TERMS

6. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet,

connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. Smartphone: A smartphone is a portable personal computer with a mobile operating system having features useful for mobile or handheld use. Smartphones, which are typically pocket-sized (as opposed to tablets, which are larger in measurement), have become commonplace in modern society in developed nations. While the functionality of smartphones may vary somewhat from model to model, they typically possess most if not all of the following features and capabilities: 1) place and receive voice and video calls; 2) create, send and receive text messages; 3) voice-activated digital assistants (such as Siri, Google Assistant, Alexa, Cortana, or Bixby) designed to enhance the user experience; 4) event calendars; 5) contact lists; 6) media players; 7) video games; 8) GPS navigation; 9) digital camera and digital video camera; and 10) third-part software components commonly referred to as "apps." Smartphones can access the Internet through cellular as well as Wi-Fi ("wireless fidelity") networks. They typically have a color display with a graphical user interface that covers most of the front surface of the phone and which usually functions as a touchscreen and sometimes additionally as a touch-enabled keyboard.

d. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

PROBABLE CAUSE

7. Pursuant to Title 18 U.S.C. Section 2258A, a provider of electronic communication services or remote computing services to the public through a means or facility of interstate commerce, such as the Internet, must report incidents of apparent violations of child exploitation statutes to the CyberTipline (CT) of the National Center for Missing and Exploited Children (NCMEC). Such a report may include the pornographic image(s) and other identifying or descriptive information.

8. On January 28, 2020, USACIDC's Major Cybercrime Unit (MCU) received NCMEC CT Reports 62776771 (Yahoo) and63568233 (Supplemental Report to CT Report 62776771) both submitted to NCMEC by Yahoo, Oath Holdings Inc. On this date, MCU also received NCMEC CT Report 24008735 (Tumblr), submitted to NCMEC by Tumblr in 2017. The CT Reports had been referred to the MCU by the Bedford County Sheriff's Office, VA.

9. According to the CT Report 24008735, a device using Internet Protocol (IP) address 73.216.74.149 had uploaded an image of child pornography on September 2, 2017. Tumblr reported the account username was "profoundyouthtaco," the account's email address was nc_mechanic@yahoo.com, and the date of the birth associated with "nc_mechanic@yahoo.com" was December 23, 1966. The Bedford County Sheriff's Office submitted a subpoena to COX Communications for subscriber information that was associated with the IP Address 73.216.74.149 at the time of the upload. COX Communications subpoena results showed that the IP address at the time of the incident was assigned to subscriber Travis Chapell with the following service address: 306 Hoke Avenue, Hopewell, VA 23860. The billing address was listed as 208 S. Mesa Drive, Hopewell, VA 23860. COX Communications

further provided information that the phone number associated with the subscriber was 804-720-2024 and the associated email address was nc_mechanic@comcast.net.

10. A review of public county records show that Travis R. Chapell ("SUBJECT") relocated to new residences numerous times between 2017 thru 2020. The SUBJECT resided at 306 Hoke Avenue, Hopewell, VA 23860 in 2017. Sometime in mid-April 2017, the SUBJECT relocated from 306 Hoke Avenue to 208 S. Mesa Drive, Hopewell, VA 23860. Public records indicate that sometime in January 2020, the SUBJECT again relocated to the PREMISES, 8900 Teakwood Drive, Disputanta, VA 23842, where he currently resides. This office coordinated with the U.S. Postal Investigative Services (USPS) which confirmed that the SUBJECT's wife submitted a family change of address to the PREMISES on January 24, 2020.

11. On January 28, 2020, I conducted a search of Department of Defense (DoD) civilian employee records and determined that the SUBJECT is a DoD government contractor currently residing at 8900 Teakwood Drive, Disputanta, VA 23842. DOD records reflect that the SUBJECT's personal phone number is 804-720-2024, and that his personal email address is nc_mechanic@yahoo.com.

12. On February 21, 2020, I reviewed the file associated with the 2017 CT Report 24008735 from Tumblr and based on my training and experience determined that the image reported by Tumblr depicted child pornography as defined by 18 U.S.C. § 2256. The file is a color digital image titled "conversation_106736321_1504356875249.jpg." The image depicts an image of a white male with an erect penis partially inserted into the vagina of a child, approximately 1-3 years of age, lying on her back. The male appears to have ejaculated inside the child.

13. On February 21, 2020, I reviewed the files associated with CT Report 62776771 from Yahoo. That CT Report showed that the images were associated with an email account of james.henry170@yahoo.com. Included in the report were 105 images and 16 videos of nude children ranging in age from approximately infant, to young teen, some of whom were engaged in sexual acts with adult male and females. These images had been transmitted via email by james.henry170@yahoo.com. The emails reported in this CT report spanned the period from December 4, 2017 thru January 10, 2020. All photos and videos were identified by my manual review and hash comparison to known child pornography. The photos and videos appear to be depictions of children between one to 12 years of age in various stages of undress, with many displaying their genitalia in a lewd and lascivious manner. Most of the depictions, both video and photos, include sexual abuse involving adults engaged in sexual acts with children, while others depicted multiple children engaged in sexual acts with each other. Some of the images are as follows:

a. A digital video file entitled "Laurie – cum.wmv" with a duration of 1 minute and 7 seconds in total length, depicting a female child, approximately 3-7 years of age, sitting down on a table, nude with an adult penis inserted into her mouth. The adult holds the penis in the child's mouth while ejaculating into her mouth and then continuing to ejaculate on her body.

b. A digital video file entitled "Vid Dad fucks girl in bathtub.avi" with a duration of 1 minute and 36 seconds in total length, depicting a female child, approximately 3-7 years of age, standing in a bathtub naked with an adult male siting on his knees naked in the bathtub holding the child. The adult male appears to be forcefully inserting his penis into the child's anus while groaning and repeatedly thrusting his penis in and out of the child. The child is heard throughout the video crying. The adult then turns the child around and begins to ejaculate on her stomach and genitalia.

c. A digital image entitled "image.149-1.jpeg" depicts a child approximately 1-4 years of age, asleep lying on her back naked from the waist down. The image is focused on the genitalia of the child which is fully exposed and further shows what appears to be ejaculate on the stomach and genitalia of the child.

d. A digital image entitled "image.32-1.jpeg" depicts a female child approximately 1 to 3 years in age, lying on her back with a pacifier in her mouth, naked from the waist down with her legs spread open in a lewd and lascivious manner. The images is focused on the child's genitalia with what appears to be a sex toy inserted into the vagina of the child.

14. In addition to the above, Yahoo submitted a Supplemental Report to CT Report 62776771 which provided the following subscriber information pertaining to the SUBJECT account james.henry170@yahoo.com:

a. The Globally Unique Identifier (GUID) for the Yahoo account is RPNMYEHLCYMVI4CVLNXO2XG2HA.

b. The user-provided name on the Yahoo account is "james henry"

c. The Yahoo account was created on October 2, 2017 at 10:54:00 (GMT) from Comcast Cable IP address 76.120.246.67, located in or around Petersburg, Virginia.

d. The phone number provided for the Yahoo account is 804-720-2024, which is the same phone number listed for the SUBJECT in DoD records.)

e. The date of birth provided for the Yahoo account is December 23, 1966. This is the same date of birth listed for the SUBJECT in DoD records. It is ***also*** the date of birth listed in the Tumblr CT Report referenced in paragraph 12 above for the email address nc_mechanic@yahoo.com.

f. The last successful login to the Yahoo account was on January 12, 2020 at 14:31:54 (GMT) from Verizon Wireless IP address 174.226.3.119 (Port 4803), located in or around Hopewell, Virginia.

g. Additional successful logins to the Yahoo account were as follows:

i. On July 23, 2019 at 17:40:23 (GMT) from Comcast Cable IP address 2601:5c5:201:2a4:6c34:d9fd:3c72:f603 (Port 50660), located in or around Hopewell, Virginia.

ii. On September 13, 2019 at 17:45:01 (GMT) from Comcast Cable IP address 73.251.67.123 (Port 51027), located in or around Hopewell, Virginia.

h. The Yahoo account was deactivated on January 13, 2020 at 16:12:55 (GMT) by Yahoo for sharing Child Sexual Abuse Images, (CSAI), as identified in CyberTip 62776771.

15. On March 11, 2020, this office received information from Verizon pertaining to Verizon Wireless Number 804-720-2024, reported in the CT Report. Based upon the subpoena returned the subscriber was identified as Travis R. Chapell, 8900 Teakwood Dr., Disputanta, VA 23842. Verizon also identified the subscriber to IP address 174.226.3.119 during the specified date in the CT report as Chappell with an address of the PREMISES.

16. On March 20, 2020, United States Magistrate Judge Roderick C. Young issued a search warrant for the email account james.henry170@yahoo.com. On April 24, 2020, Yahoo Search Warrant Returns were received by this office. Images and videos previously reported by Yahoo in the CyberTip 62776771 matched images and videos provided in the search warrant return. There were also additional images of child pornography received by the email account.

17. On April 25, 2020, SA Roelofs reviewed over the Yahoo Login Activity Summary provided from the Yahoo warrant return. The information contained within the login activity summary indicated that a user logged into the james.henry170@yahoo.com account from March 31, 2019 to January 12, 2020 from 39 different IP addresses. Based on analysis of the IP

addresses, 26 of the 39 IP addresses were identified as being provided by the Internet Service Provider (ISP) Company CELLCO. CELLCO is a partnership of Verizon Wireless and provides wireless voice and data services on behalf of Verizon. Additionally, a search of Federal Communication Commission (FCC) records further revealed that a CELLCO cellular tower resides just 7.3 miles from the subject premises. In my training and experience, based on the majority of the ISP data originating from CELLCO, it is likely that the subject used his cellular phone to login into the james.henry170@yahoo.com account given that more than half of the logins were done using a cellular IP address.

18. Additionally, emails sent and received by the email account included messages discussing the trading of child pornography and engaging in sexual acts with children. Some of the messages contained within the Yahoo warrant Return from the email account are as follows:

a. On March 29, 2018, SUBJECT emailed User 1 with a gmail.com account:

   i. "dude....i still look at your daughters pics you sent....man i wish i was able to give her my cock. i cant wait to see more pics of her. just in case you forgot my name in chat room here it is older male 4 yngr hope ya enjoy these pics as well....dont stroke to hard to them".

b. On March 30, 2018, SUBJECT emailed the User 1:

   i. "dayummmmm tight ass....were you able to get your cock into her ass? omg i would have loved to try. and that pussy looks to be nice and smooth....omg your lucky dude....wish i could get ahold of your wife and daughter as you watched me with them if you got any more of you and wife...send them..id love to see you fucking her or her sucking you. hope you enjoy this vid".

c. On December 5, 2019 SUBJECT emailed another individual, User 2:

   i. "I was thinking the same thing. show you the pics...you sucking my cock. the thought of an older man sucking me off and not looking for anything in return really got me going. shame I don't know of a young girl we could have with us to use. hell if you know of one you can bring with you..bring her...we can do her at same time or watch the other use her".

d. On December 26, 2019 SUBJECT emailed User 2:

   i. "i cant wait until jan....I want you to look at some pics and stroke my cock as you tell me to think of the girl as your granddaughter...then you slide down and start to stroke my cock more and then to take it into your warm wet mouth".

e. On 27 December 2019, SUBJECT emailed another account, User 3:

   i. "this is a good date for me as well. id love to fuck you and your daughter".

f. On December 30, 2019, User 3 responded:

   i. , "Hi, Were you still interested in meeting".

g. On January 10, 2020, SUBJECT responded to User 3:

   i. "remind me your information. where your from. your age and daughter information".

19. On 4 May 2020, HSI Special Agents again conducted physical surveillance at the PREMISES. The SUBJECT was observed leaving the PREMISES at 4:30pm.

COLLECTORS OF CHILD PORNOGRAPHIC MATERIAL

20. Based upon my training and experience in child sexual exploitation and child pornography investigations, and having worked with other experienced law enforcement officers in child exploitation investigations, I know the following:

a. Individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect their collections of illicit materials from discovery, theft, and damage. The known desire of such individuals to retain child pornography together with the sense of security afforded by using computers, provides probable cause to believe that computer images, especially child pornography and erotic nudity involving minors, will be retained by the collector indefinitely. These individuals may

protect their illicit materials with passwords, encryption, and other security measures. These individuals may also protect their illicit materials by saving them on movable media such as memory cards, memory sticks, CDs, DVDs, flash memory, thumb drives, and removable hard drives, which can be easily secreted as they are very small in size -- often as small as a postage stamp -- or sent to third party image storage sites via the Internet.

b. Individuals who maintain images of child pornography often maintain these images on cameras, film, video cameras, videos, computers, and other photographic equipment.

c. Individuals who collect child pornography will frequently conceal their digital media devices on their person so as to conceal their activities from family members and protect their digital content. These individuals may also store the information in their mobile telephone to allow remote access to their collections while travelling. Media storage devices are frequently marketed for their portability and can come in various shapes and sizes to include key chains, sunglasses, or toys.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

21. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PERSON and PREMISES in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information pursuant to Rule 41(e)(2)(B).

22. *Probable cause.* I submit that if a computer or storage medium is found on the PERSON and PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is

typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

23. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PERSON and PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial

evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether

data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer it will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

24. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make

an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

25. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

26. Because there is a potential for several people sharing the PREMISES as a residence, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

UNLOCKING THE DEVICE(S) WITH BIOMETRIC FEATURES

27. The search warrant I am applying for would permit law enforcement to obtain from Travis R. CHAPELL the display of physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) in order to unlock devices subject to search and seizure pursuant to this warrant. I seek this authority based on the following:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many

electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. Apple offers a facial recognition feature called "Face ID." During the Face ID registration process, the user holds the device in front of his or her face. The device's camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Face ID.

d. If a device is equipped with an iris recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

f. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices, including a cellular phone, will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, based on my training and experience, law enforcement personnel may not be able to access the data contained within such device(s) without the use of biometric features.

g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

h. Accordingly, I am requesting that, if law enforcement personnel encounter device(s) that is or are subject to seizure pursuant to this search warrant and may be unlocked using one of the aforementioned biometric features, the search warrant I am applying for would permit law enforcement personnel, acting as soon as reasonably practicable, to (1) press or swipe the fingers (including thumbs) of Travis R. CHAPELL, to the fingerprint scanner of the device(s); (2) hold the device in front of the face of Travis R. CHAPELL and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search its contents as authorized by this warrant.

CONCLUSION

28. Based on the forgoing, I request that the Court issue a search warrant under Fed. R. Crim. P. Rule 41 for the PERSON and PREMISES described in Attachment A and seize the items described in Attachment B.

Respectfully submitted,

Michael J. ~~Roelofs~~
Special Agent
U.S. Army Criminal Investigation Division
Major Cybercrime Unit

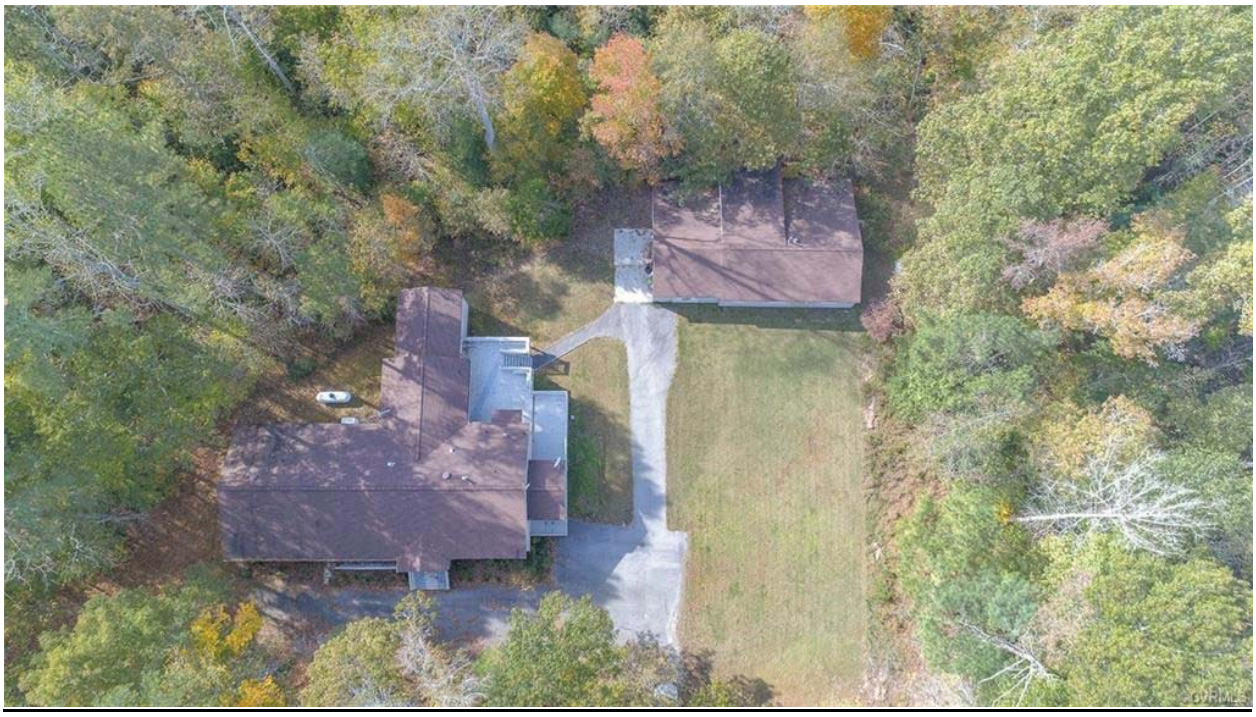
Subscribed and sworn to before me on May 7, 2020 at Richmond, Virginia.

/s/
Roderick C. Young
United States Magistrate Judge

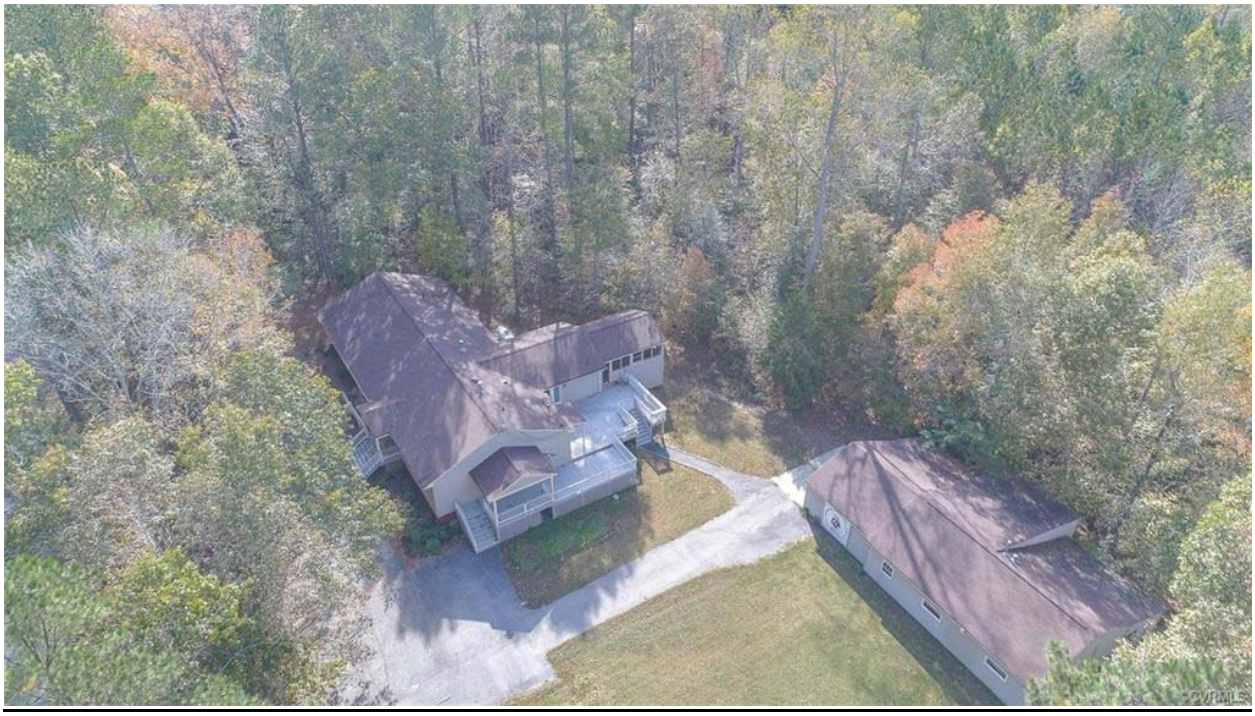
ATTACHMENT A

Property to Be Searched

1. This warrant applies to a search of the PERSON of Travis R. Chapell and the PREMISES located at 8900 Teakwood Dr., Disputanta, VA 23842, including all structures on the property.
2. This search warrant authorizes the use of biometric methods as described in Paragraph 27 of the Affidavit in Support of an Application for Search Seizure Warrant.




HAIL



ATTACHMENT B

1. All records relating to violations of Title 18, United States Code, Sections 2252 and 2252A, Receipt, Distribution and Possession of Child Pornography, including:

i) Computers, mobile devices, or storage media used as a means to commit the violations described above.

ii) Records and information identifying who used, owned, or controlled the device at the time the things described in this search and seizure warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents browsing history, user profiles, email contacts, "chat," instant messaging logs, photographs, and correspondence;

iii) records and information relating to software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iv) records and information relating to the lack of such malicious software;

v) records and information indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to be computer user;

a. records and information relating to the computer user's state of mind as it relates to the crime under investigation;

b. records and information relating to the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

c. records and information relating to counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

d. records and information relating to the times the COMPUTER was used;

e. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

f. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

g. records of or information about Internet Protocol addresses used by the COMPUTER;

h. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

i. Contextual information necessary to understand the evidence described in this attachment.

4. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer," includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium," includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, DVDs, and other magnetic, electronic, or optical media.